

4 EPA TECHNICAL REFERENCE MODEL

The Environmental Protection Agency (EPA) Technical Reference Model (TRM) describes the association of information technology (IT) services within three major areas that comprise the EPA's Enterprise Technology Architecture (ETA). The TRM also diagrams the relationship between the three major areas and the major services. The usefulness of this model is to compartmentalize the wide array of information technology into manageable components and to guide the development of the target ETA. The diverse groups at EPA applying information technology to their business needs can now reference a common model of their information technology and a common vocabulary, thus improving the representation of these groups in the target technology. This model also provides a springboard for coordinating the research of information technology.

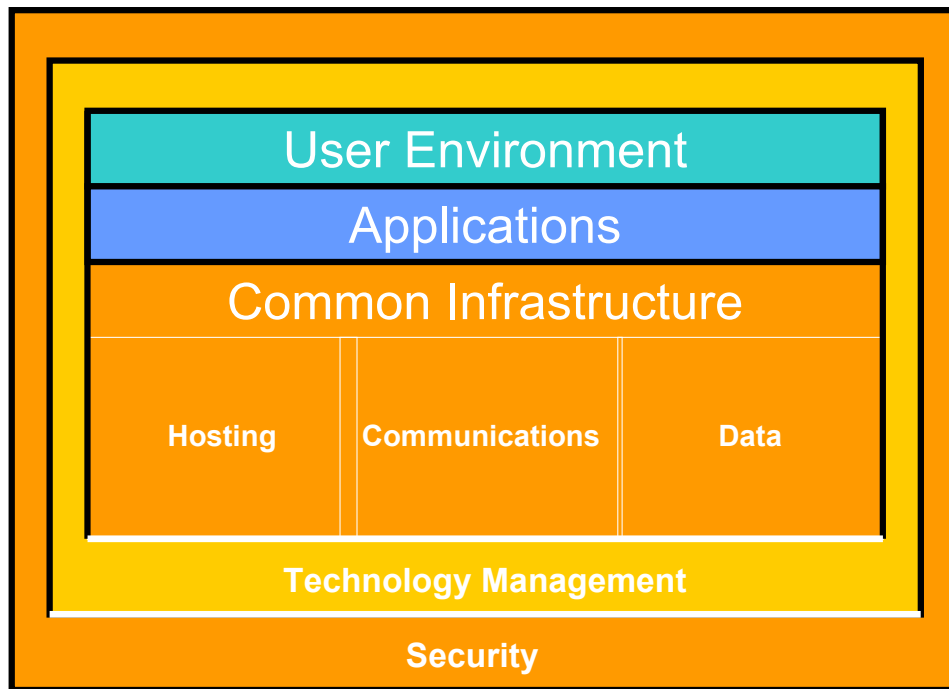
4.1 EPA TRM Design

The EPA TRM defines three major areas that collectively describe the EPA Enterprise Technology Architecture. These three major areas are the User Environment, the Applications, and the Common Infrastructure. Figure 4.1 below illustrates these three areas and their interfaces. The User Environment and Applications provide end user services and application services. The Common Infrastructure area is further divided into five major services which are: 1) Hosting, 2) Communications, 3) Data, 4) Technology Management, and 5) Security. Figure 4.1 below illustrates the seven major services and their interfaces.

The TRM diagram layers the services in a meaningful fashion. Each distinct layer is separated by a dark line. The top layer consists of End-User Services and its position serves to emphasize that the other layers exist to support the end-user. The second layer is Application Services which provides the end-user with the EPA's mix of environmental and business application services. The third layer is the Common Infrastructure (divided with white lines) which makes possible the operation and communication of the Application Services with the end user and with the Agency's data stores. See Figure 4.1 below to review the interfaces of the various services.

The TRM diagram has been designed to emphasize the role of Technology Management and Security in relation to the other services, even though they are part of the Common Infrastructure. The reader should note that Technology Management surrounds the other services since it is necessary to all these services given the complexity of today's information technology. Security has been designed to surround Technology Management since secure technology is currently the overriding factor for technology implementation and is a requirement in all the other services.

Each of these major services and their associated minor services are discussed in detail in the following sections.



USEPA - © 2002

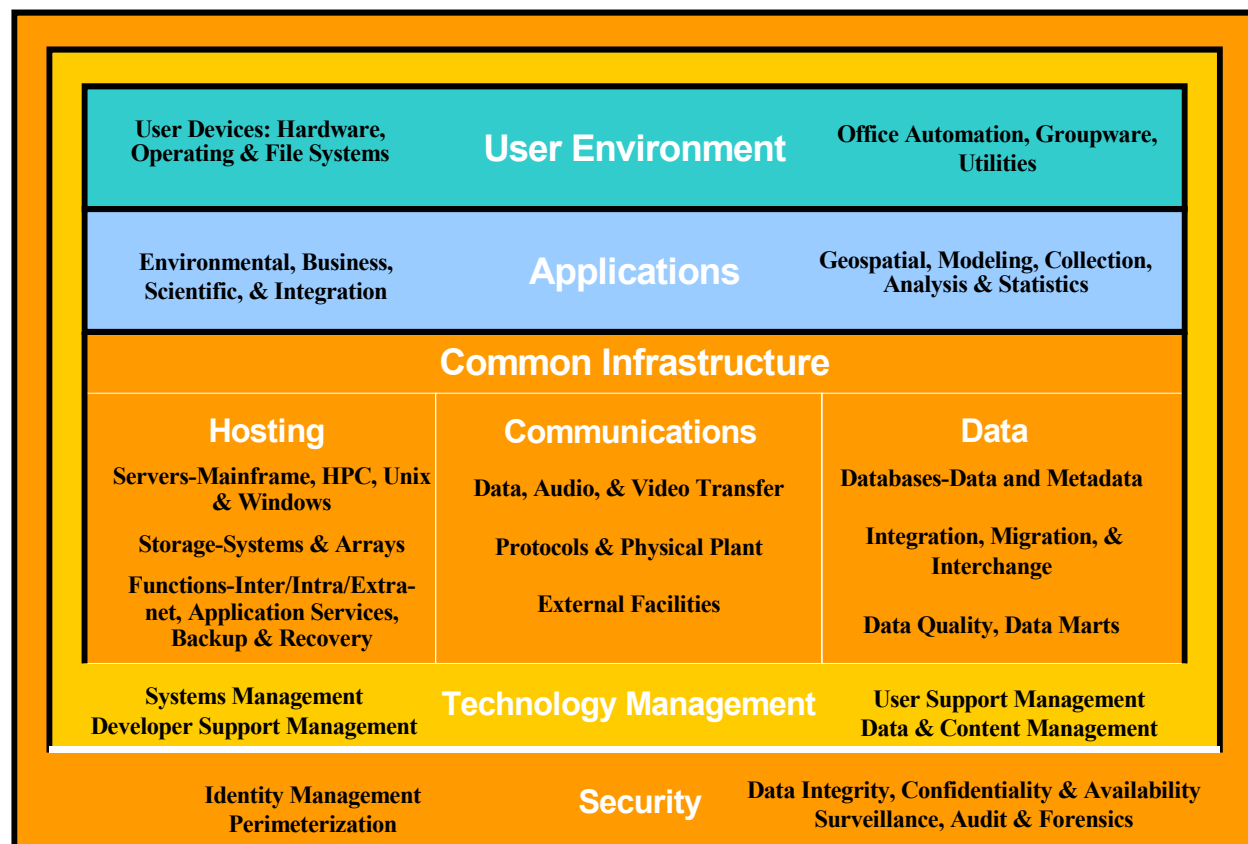
Figure 4-1. USEPA Technical Reference Model

4.2 EPA TRM Detail

The initial delineation of the seven major service areas, identified in Figure 4-1, provides a framework that enables a basic viewpoint and understanding of EPA technology architecture.

The EPA TRM high-level or major service areas are each associated with lower-level services (i.e., minor services). Some of these minor services are also associated with a finer level of detail (e.g., Systems Management). The purpose of this section is to define these minor services so that readers and users of the TRM have a good understanding of the services and will contribute to the validation of the definition and/or the modification of the definition to accurately reflect the particular use of technology at EPA. As new technologies are implemented, the reader may also discover that an area of technology is missing a service designation and that a service category needs to be created. The TRM is a living document that will be modified to reflect the needs of EPA and the rapid changes occurring in information technology.

Figure 4-2 below provides a detailed view of the TRM with the major and minor services. The seven major service areas and their minor services are considered in the following sections.



USEPA - ©2002

Figure 4-2. USEPA Detailed Technical Reference Model

4.2.1 User Environment

In the EPA TRM, User Environment is defined as the sum of all hardware and software components required to provide access to EPA information for all levels and types of users. EPA's User Environment is categorized into five minor services which are fully described below.

4.2.1.1 User Device: Hardware and Interfaces

User Device Hardware and Interfaces are the technology components that provide the end-user with the physical devices necessary to connect, communicate and process information. The device hardware includes digital information processors such as the Personal Computer (PC), scientific Workstation, Mobile Computer, Personal Digital Assistant (PDA) and Mobile Phone. Interfaces include the hardware for connecting to a

network such as the Network Interface Card (NIC) and the hardware the user needs to communicate with the computer such as the optical mouse or the speech recognition processor and microphone. Other interfaces include scanning devices, pen tablets, keyboards, and display screens.

4.2.1.2 User Device: Operating and File Systems

User device operating and file systems provide the services needed to operate and make the user device hardware intelligent and capable of storing and retrieving information. Operating systems include the many versions of Microsoft Windows, Unix, and Linux that are available for user devices.⁶ Operating systems provide an interface between the application software and the hardware platform. Operating System Services can include the following: kernel operations, real-time extensions, clock/calender services, fault management, access management, shells, utilities, application program interfaces (APIs) and File System Services. Most File System Services are embedded in the operating systems but some are not. New types of File System Services are provided by storage Web sites, by optical devices, and by Universal Serial Bus (USB) flash drives which store files on removable microchip file systems.

4.2.1.3 Office Automation

Office automation software for common office functions, such as word processing, is used in day-to-day operations at EPA. This software can include: Spreadsheet, Project Management, Calculation, Presentation and Word Processing Services.

4.2.1.4 Utilities

This category includes software that makes the end-user's processing environment more efficient and productive. Examples of such tools include utilities for unused file clean-up, disc defragmentation, file transfer, file compression, system monitoring and searching.

4.2.1.5 Groupware

The services provided under Groupware include those that allow end-users to collaborate with peers inside and outside EPA. Groupware includes software for Email, Calendaring, Conferencing, and Instant Messaging Services. Groupware's most prevalent service is the World Wide Web (WWW) browser which provides a graphical interface to information and services available from all over the world.

4.2.2 Applications

EPA's Applications Service is categorized into 13 minor services which are fully described below.

⁶ Unix and Linux Operating Systems are only supported in limited setting and primarily for statistical, visualization and/or GIS applications.

4.2.2.1 Environmental

Environmental applications provide the Agency with a service to assist its mission to protect the environment. These applications measure, process, analyze and store for use the data that determine whether mandates are being met and the quality of the environment is changing. Examples of these applications include: SDWIS (Safe Drinking Water Information System), RCRIS (Resource Conservation and Recovery System), CLP (Contract Laboratory Program) and PCS (Permits Compliance System).

4.2.2.2 Business

Business Application Services are primarily composed of Administrative applications that provide the Agency with the software services to conduct the internal financial, personnel, and organizational functions required for the success of any large organization. Business Application Services may also include applications that provide necessary business functions such as measuring the effectiveness of project funding against project output. Examples of EPA Administrative applications in this category include: EPAYS (EPA Payroll System), ICMS (Integrated Contract Management System) and IFMS (Integrated Financial Management System).

4.2.2.3 Scientific

This service is a larger category for the myriad group of applications that help EPA to do its science work, such as collecting, validating, analyzing, condensing, and displaying data and developing forecasts. Many of the science applications fall into other minor service categories that follow.

4.2.2.4 Integration

Integration Services provide for the applications that make possible Enterprise Application Integration (EAI). Specifically, this includes middleware products that interface transaction processing between differing applications and platforms (e.g., IBM MQSeries, however, EPA does not use MQSeries) or Web Services that provide application integration (e.g., WebSphere, SeeBeyond, which EPA plans to use) through the use of the standard Web browser interface.

4.2.2.5 Document Management

Document Management Services provide a procedure for archival of EPA information. The EPA archives annually an average of 11,442 cubic feet of paper which is roughly equivalent to 1.583 Terabytes of text data.⁷ Different service offerings have been considered for this technology service such as providing a user with the ability to designate Email for automatic archival.

⁷ *Records Management Storage Architecture Methodology Report*, USEPA-NTSD, September 1999.

4.2.2.6 Workflow

Workflow Services provide a means for routing documents and files automatically to the person or organization responsible for the next step in processing. Examples of this service include time sheet processing and E-forms.

4.2.2.7 Collaboration

Collaboration Services provide support for the online and often real-time capture and processing of information exchange between members of a user group working together on a project but physically not together. Examples of applications for this service would include Sametime, a COTS package from Lotus/IBM. This service would include central hosting support as well for Email and Calendaring as well as for future desktop video-conferencing.

4.2.2.8 Geospatial

Geospatial Services provide applications that process data spatially so that environmental information has a "space and a place." This service includes applications such as: OMS (Ozone Mapping System), MAIA (Mid-Atlantic Integrated Assessment) and EnviroMapper.

4.2.2.9 Analysis

Analysis applications provide environmental researchers with tools to qualify raw data that has been collected and to condense or combine data as required by the project. Analysis software helps to detect and remove "outliers," i.e., raw data that is outside of the valid range of environmental norms, and to reduce raw data into averages that are usable by researchers.

4.2.2.10 Modeling

Modeling applications provide environmental researchers with tools to develop digital representations of reality based on data so that scenarios can be evaluated virtually and conclusions or predictions can be made. Modeling applications provide techniques to predict future behavior of environmental systems and anticipate the consequences of change. Once a model is formulated to represent real environmental conditions, predictions are made and then the model is validated or improved as additional measured data becomes available. Many of EPA's modeling applications run on the High Performance Computing platform, Unix workstations and Linux clusters.

4.2.2.11 Statistics

Statistics Services provide applications (both COTS and custom-developed) that compute numerical profiles or descriptors of sets of numbers according to the theories of mathematical analysis and probability. In environmental science, a statistical descriptor could be the mean concentration of a pollutant or the standard deviation of hydrocarbons in samples of air. This service provides EPA users with applications such as PC and Linux SAS and SAS on the Enterprise Computing platform.

4.2.2.12 Lab Science

Lab Science Application Services are those which support the operation of laboratory work to research environmental questions such as toxicity of chemicals. These services support animal experiments, equipment calibration, chemical identification, etc.

4.2.2.13 Data Collection

Data Collection Services involve computing applications developed or purchased to acquire measured data from instruments, either on-site or remotely, or to receive data from other data submitted. The EPA measures environmental variables in a number of ways using sophisticated instruments that feed data into data loggers and real-time computers. Fairly sophisticated data collection applications are used to interface with instruments. Data Collection Services may also provide applications to interface with other data generators outside of EPA, such as city/county monitoring stations operated by State environmental offices. These applications act as middleware to obtain data that has been collected and stored in non-EPA systems.

4.2.3 Hosting

In the EPA TRM, Hosting is the service that provides the platforms and systems to run the Applications of the Agency and to store and maintain the information processed through these systems. The EPA Hosting Service is categorized by the TRM into seven minor services which are described in the following subsections.

4.2.3.1 Enterprise Server (Mainframe)

The Enterprise Server platform provides for running EPA's enterprise-wide applications (see Environmental and Administrative above). This service also provides for hosting "individual" applications that process data for a particular environmental project. "Customers of this service receive use of an IBM Enterprise Server that supports large-scale data processing and provides information vital to accomplishing the Agency's mission. The Enterprise Server provides resources to over 9,000 registered users. An operations staff continually supports the Enterprise Server to ensure that it is operational at least 99% of its scheduled hours of operation."⁸ The Enterprise Server operates 24 hours a day, 7 days a week. This service supports the ADABAS database system and the DB2 relational database system, SAS, a complete set of third party software, and data backup and restoration.

4.2.3.2 High Performance Computing

The High Performance Computing (HPC) Platform Service supports high-performance computing, scientific visualization, and computation sciences service on state-of-the-art high performance computers (vector and parallel). "High performance computing combines very powerful computer processors, massive amounts of data, high speed networks, and mathematical models to simulate global and regional environmental

⁸

WCF Services: <http://cfint1.rtpnc.epa.gov/ntsdWeb/currentfyservices/qa/qa.cfm>

conditions. Researchers and policy analysts create scientific visualizations from data generated by computer simulations, data collected from monitored data, or text-based data and information. The visualizations are generated from commercial off-the-shelf software or from customized software developed by EPA's Scientific Visualization Center. The scientific visualizations can be displayed on desktops, servers, or through Web-based applications."⁹

4.2.3.3 Central Unix & Windows Servers

The Central Unix & Windows Servers Service (also referred to as Central Client Server Systems) provides platform support for EPA's Oracle databases and other Unix-based components supporting EPA's Public Access, Intranet, and Extranet applications.¹⁰ This service also includes support for Windows platform servers supporting Web application components such as Domino, ColdFusion, and ArcInfo GIS Mapping applications. This service includes hardware, software, and operations and technical support staff tasked to operate EPA's centrally managed Unix/NT systems 24 hours a day, 7 days a week. This service hosts EPA's Public Access Web site and EPA's Intranet Web sites, and provides development and staging systems for Web site developers. Many of EPA's most visible applications are run using this service.

4.2.3.4 Distributed Unix, Netware and Windows Servers

Distributed Computing Services provide specialized support for computing platforms that are physically or logically dispersed geographically among computer systems on a wide area network. These servers are typically used to support local area networks which connect groups of users that are geographically close. These servers provide localized application hosting, data storage, file & print services, security monitoring and support for technology management software. Distributed systems support services includes support via Unix, Linux, Novell, Windows 2000 Server, and Windows NT Server operating systems and provide standard configuration documentation that systems must comply with before they can attach to the Wide Area Network and communicate within the Agency. Specialists provide help desk support for Unix, Linux, Novell, Windows 2000 Server, and Windows NT Server.¹¹

4.2.3.5 Storage Systems and Arrays

This service includes the support for centrally storing and managing data for transparent retrieval, high-availability, and long-term retention. Each platform service at EPA has its own particular storage architecture that includes magnetic disc storage, disc arrays, magnetic tape, and magnetic tape juke boxes (tape silos). Though some sharing of resources does occur between platforms at EPA, the Enterprise Computing, HPC, Central Unix and Windows, and Distributed Unix and Windows platforms all currently provide and manage their own systems for this service which includes managing storage allocation per user accounts. File servers

⁹ WCF Services: <http://cfint1.rtpnc.epa.gov/ntsdWeb/currentfyservices/sc/sc.cfm>

¹⁰ WCF Services: <http://cfint1.rtpnc.epa.gov/ntsdWeb/currentfyservices/uc/uc.cfm>

¹¹ WCF Services: <http://cfint1.rtpnc.epa.gov/ntsdWeb/currentfyservices/u9/u9.cfm>

(Netware, NT and Lotus Notes) that are geographically dispersed each have their own storage subsystems to support their user base.

4.2.3.6 Backup and Recovery

This service provides for maintaining a redundant copy of the storage system data available on the various hosting platforms and restoring the data should an on-line storage system fail. This service also provides recovery of data that was erased through human or system error. Currently, each hosting platform operates its own separate Backup and Recovery Service to provide for data security.

4.2.3.7 Disaster Recovery

This service provides restoration of data and computing platforms in the event that a disaster disables one or more critical systems. Disaster Recovery Services include provisions for offsite storage of data and availability of offsite computing capacity. This service is invoked only under certain extreme situations where the normal hosting services are interrupted for an extended period of time.

4.2.4 Communications

The EPA Communications Service is categorized into five minor services which are fully described below.

4.2.4.1 Data, Audio and Video Transfer

This service involves providing the bandwidth that is appropriate for transferring character data, audio data (streaming audio, Voice over IP), and video data (streaming video, desktop teleconferencing, etc.) in a time-sensitive manner. This service includes measuring communication loads, load balancing, and forecasting upgrades to the physical plant.

4.2.4.2 Protocols

This part of the Communications Service involves the support of protocols for the transport of data, the most important being the Internet Protocol (IP). Included are local area network protocols such as IPX/SPX, IP, TCP(Transmission Control Protocol)/IP, NetBUI, HTTP(Hypertext Transfer Protocol), FTP(File Transfer Protocol), and other protocols covered under IP security (IPSEC) such as VPN (Virtual Private Network). This service ensures that data is encoded before transmission such that it can be compatible across the Agency infrastructure and the outside world.

4.2.4.3 Physical Plant

The Physical Plant Service includes the communication infrastructure components that the Agency provides to make the wide area, metropolitan area, and local area networks interconnect in a reliable and secure fashion. To provide this service, the physical plant includes fiber optic and copper cabling, ethernet coaxial cable segments, twisted pair copper wiring, network switches, network bridges, and network gateways. These services support the transport of data, in whatever format, using the Internet Protocol.

4.2.4.4 External Facilities

The EPA provides a large part of wide area network connectivity through leased T1, T3, and PSN/ISDN lines. These facilities are not owned or maintained by EPA but are leased as a managed service from external providers. The quality of the service is supervised by EPA and the service these external facilities provide is critical to the operation of EPA's infrastructure. External facilities for communication include EPA's connections to the Agency Internet Service Providers (ISP) and metropolitan and wide area line connections between Agency communication hubs.

4.2.4.5 Remote Sensing

This service provides the communications link to remote sensing devices or measuring instruments located in remote geographic areas or separated from the personnel responsible for their functioning. The communications link may be through dial-up or leased telephone lines, wireless, or through custom cable installation.

4.2.5 Data

The EPA Data Service is categorized into six minor services which are fully described below.

4.2.5.1 Databases for Data and Metadata

Database Services provide the capability to store, retrieve, organize, and manipulate data in a database management system (DBMS). These services provide a consistent programming interface to the developer while segmenting access to data from a variety of sources. Query-processing Services provide for interactive selection, extraction, and formatting of stored information from files and databases. The platform that runs a DBMS is relegated in the TRM to the Hosting Service, and the operation of the DBMS including its maintenance, upgrades, partitioning, user accounts, and documentation is relegated to the Data Management Service under Technology Management.

Databases provide structured storage for both the Agency's data and metadata. The Agency's data includes large stores of information on the ecological environment, chemicals, experiments, monitoring, etc. and also include collections for releasing data to the public. The Agency's metadata is inventory of its data, i.e., it provides information about the data collections the Agency is accumulating. Metadata is also one of the tools being used to enable the integration of data. Both data and metadata are maintained primarily in database systems provided by this service.

4.2.5.2 Data Integration

The Data Integration Service is receiving special prominence as the Agency wrestles with data collections that exist in various organizational stovepipes and that may have varying parameters that make joining the data difficult. As a starting point, data integration requires identifying the parameters of the various data collections through the use of metadata and then determining what level of integration can occur. This service

is also concerned with the logistics of handling large data collections and whether to consolidate them logically or physically.

4.2.5.3 Data Migration

This service provides for moving data from one DBMS environment to another DBMS environment. Migration may involve moving data to a new hardware platform, new DBMS software, or both. Migration Services can be small-scale, such as migrating a single database, or large-scale, involving many databases or data collections. Migration Services also include converting data into some common format that can be output from an old database and input into a new database. Since the new database may be organized differently, it is often necessary to write a program that processes the migrating files.

4.2.5.4 Data Interchange

The Data Interchange Service provides specialized support for the access of information between applications and/or between internal and external user environments. This service supports the import and export of data to and from DBMS systems and the format translations that may need to occur to make data readable by an end-user or by another application. Interchange Services apply also to document exchange between computer systems and between document processing software.

4.2.5.5 Data Quality

The Data Quality Service is intended to ensure that data stored in the Agency's collections conforms to standards for accuracy, data definition, and error rates. Data Quality Service also includes validation which applies business rules to check data content. The Data Quality Service also qualifies data for entry into a data warehouse to avoid the hazards of storing and later disseminating incorrect data.

4.2.5.6 Data Marts

The Data Mart Service is the area of information technology that will make it easier for Agency stakeholders and the general public to access information relevant to the environment. This service primarily summarizes data in time and space from more complex detailed data sets. This service provides the "kiosk" for environmental information, including the Web application interface and the data warehouse. The Agency is transitioning to this service as a target architecture away from the stovepiped information delivery provided through the Applications Service.

4.2.6 Technology Management

Information systems are composed of a wide variety of diverse resources that must be managed effectively to achieve the goals of an open system, standards-based environment. While the individual resources may differ widely, the abstraction of these resources as managed objects allows for their treatment in a uniform manner. The basic concepts of management, including operation, administration, and maintenance, may then be applied to the full suite of technology components along with their attendant services. The EPA Technology Management service is categorized into five minor services which are fully described below.

4.2.6.1 Systems Management

Systems management functionality is divided into the following elements: Usage Monitoring, Capacity Planning and Forecasting, Network Management, Change Management, Configuration Management, and Asset/Inventory Management. These elements of the Systems Management service are described individually in this section.

4.2.6.1.1 Usage Monitoring

This service measures system resource utilization on the various hosting platforms provided by the Agency. This service also measures usage of the Agency's Web services, primarily the Public Access (Internet) Web sites, to collect statistics on how many pages are downloaded from the different sites and how much data is transferred each day. Web site usage also records from where page requests are made. Daily usage is combined into monthly averages and is useful for Capacity Planning.

4.2.6.1.2 Capacity Planning and Forecasting

This service takes information on system resource utilization and applies statistical trending techniques to provide short term (Planning) and long term (Forecasting) estimates of resource needs for the Agency's Hosting platforms. Currently, this service is applied primarily to the Enterprise (mainframe) Server and the large Unix platforms. An example of Capacity Planning is to trend the CPU (Central Processing Unit) usage of the major applications running on the mainframe and then to determine if additional processing capacity will need to be added in a few months. An example of Forecasting is to project the trends on CPU and storage utilization to determine if major system changes will be necessary in a two-year time frame.

4.2.6.1.3 Network Management

This service handles the complex task of ensuring that EPA's network systems are functioning well. This service monitors network nodes for traffic density, re-routes network traffic in the event of a network component failure, monitors the type of data being transported, and in general, plans for the availability and bandwidth of the Agency's Wide Area Network, Metropolitan Area Network, and the connections to the Internet.

4.2.6.1.4 Change Management

This service provides for the orderly and planned execution of changes to computer system hardware and software, including processing capacity, storage capacity, peripheral changes, and operating system migrations. This service not only determines if and when changes can and should occur, but also notifies the user community in advance to provide an orderly transition with minimal disruption.

4.2.6.1.5 Configuration Management

This service provides for arranging systems and system resources to make them more efficient and effective and to ensure that they meet the needs of the user community. This service provides the testing and

documentation of hardware and operating systems to define the proper operating configuration within the Agency's IT infrastructure so that system conflicts and security concerns can be addressed. This service may also involve placing and removing computer resources and deciding which resources should be allocated.

4.2.6.1.6 Asset/Inventory Management

This service provides for the accounting and allocation of the Agency's computers and peripherals. The output of this service is useful for depreciating resources and planning capital improvements, as well as tracking equipment and licenses for hardware and software.

4.2.6.2 Developer Support Management

This service provides the tools and resources needed by the application development community at EPA. The developers require specialized IT software and systems to coordinate their efforts. This service includes software for code management, code libraries, code life cycle management tools, software emulation tools, CASE tools, object-oriented designer tools, code generators, and automated testing.

4.2.6.3 User Support Management

User Support Management functionality is divided into the following elements: Help Desk Support, Software Distribution, and Problem Management.

4.2.6.3.1 Help Desk Support

This service provides the function for handling the user community's IT problems and questions and for tracking the resolution of the problems. This service is provided at EPA by the Technical Support Center (TSC). The mission of the TSC is to be the central point of contact for technical information and assistance for computer systems, networks, and applications supported by the Agency, to assist the integration of new and target technologies into the Agency, and to act as the user community's advocate by increasing visibility to user issues and by disseminating information relevant to other services.

4.2.6.3.2 Software Distribution

This service is intended to provide for the efficient and effective delivery of software to the distributed computing resources of the Agency, including approximately 24,000 personal computers and the local area network servers that support the user environment. This service is preferably transparent to the user, but at the very least, should provide a more cost-effective approach to updating software in the distributed computer environment.

4.2.6.3.3 Problem Management

This service is available as part of Help Desk Support to track and manage problems with the Agency's IT resources. This service provides for an automated tracking database that will escalate problems that are not resolved and prioritize problems according to need.

4.2.6.4 Data Management

This service provides for the administration, planning and architectural control associated with the Agency's centralized data systems. This service includes managing the DBMS, including its maintenance, upgrades, optimization, partitioning, user accounts, and documentation, while the databases and their maintenance are part of the Data Service in the TRM, and the platform that runs a DBMS is relegated in the TRM to the Hosting Service. This service also includes the planning, distribution, and control of Document and Records Management applications.

4.2.6.5 Content Management

This service is intended primarily to manage the Agency's large and increasing Public Access Web presence, though other types of content may be included in the future. The Web presence of EPA is the main external view of the Agency, and as such, needs to be managed to reflect the mission goals of EPA and to project a consistent and uniform view from a very diverse group of Web site developers and content providers. This service includes making an inventory of Web site content and providing the software and methodology to allocate content and keep it current. Monitoring compliance with the American Disabilities Act for Web page construction is also part of this service.

4.2.7 Security Service

The TRM Security Service allows groups of users to share information systems and data while guaranteeing the security of the computers, networks, and data transported to users. The Security Service is categorized into six minor services which are fully described in the sections below.

4.2.7.1 Identity Management

This service primarily provides identity administration and authentication mechanisms for the Agency's IT infrastructure. Identity administration includes the registration process for authorized users of EPA systems and the serving of identity information to the different control facilities. Administration also includes the synchronization and optimization of Agency directory systems. Authentication includes identifying users when they try to access an EPA information resource. Although this service applies primarily to managing user identities, it may also apply to the identity management of computer systems. DNS, which is a centrally managed service for the network, currently identifies all EPA server-based computer systems.

4.2.7.2 Perimeterization

The Perimeterization Service ensures that unauthorized data are not allowed to be transferred across a perimeter surrounding an IT resource or process. This service includes external and internal perimeterization. External perimeterization refers to maintaining a perimeter between the EPA network and the outside world (primarily the Internet), while internal perimeterization refers to a perimeter between one subset of the EPA internal network and the rest of the internal network.

4.2.7.3 Data Confidentiality and Integrity Assurance

This service provides the necessary measures to ensure that data/information cannot be read or altered by unauthorized personnel while stored in the Agency or during transmission between source and destination. This service includes encryption of data, encryption of communication paths, and processes to provide proof of the integrity of data (i.e., that data are not altered or destroyed in an unauthorized manner). This service applies to data in permanent data stores and to data in active use.

4.2.7.4 Data Availability Assurance

This service provides measures to ensure that data/information remains in existence and available to users when they require it. This service includes policies and planning to ensure backup/restore of data, disaster recovery for data and critical business systems, redundant paths for WAN communications, and fail over clustering support for Email and File and Print systems. This service also includes a number of Continuity of Operations Plan (COOP) initiatives.

4.2.7.5 Surveillance

This service provides systems and procedures to actively monitor network traffic and activity in order to identify attempted and/or successful intrusions or compromises to the network. This service also includes periodically monitoring network and desktop computers to ensure that they conform to security requirements.

4.2.7.6 Audit and Forensics

This service consists of measures to ensure compliance with the Agency's security program and to review records or prior network traffic and activity in order to reconstruct previous attempted and/or successful intrusions or compromises. This Audit Service includes the confirmation of operating computer environments, software (including custom developed applications) environments, and performing internal and external vulnerability assessments. The Forensics Service includes analysis of logs, intrusion reconstruction, investigations and incident response.